AMENDMENTS TO THE CLAIMS

Claims 1-7, 9-24, and 26-43 are pending in the instant application, of which claims 1-7, 9-24, and 26-28 have been rejected. Claims 29-43 have been allowed. Claims 1-28 have been cancelled.

The Applicant requests reconsideration of the claims in view of the following amendments reflected in the listing of claims.

Listing of claims:

1. – 28. (Cancelled)

29. (Previously Presented) A method for establishing secure access to a media peripheral in a home via a node in a communication network, the method comprising:

acquiring by the node, security data associated with the media peripheral;

searching by the node, for a previously acquired security data associated with a location of previous operation of the media peripheral;

if said previously acquired security data is not found:

communicating between the node and the media peripheral, information associated with the media peripheral, while the media peripheral is located in the home; and

if said previously acquired security data is found:

utilizing by the node, said acquired security data associated with the media peripheral and said previously acquired security data to

facilitate secure communication between the media peripheral in the home and the communication network;

acquiring at least one identifier associated with a location of previous operation of the media peripheral;

validating said acquired at least one identifier based on said previously acquired security data, prior to communicating over the communication network; and

if said acquired at least one identifier is valid, registering the media peripheral for subsequent operation while being located in the home.

30.   (Previously Presented) The method according to claim 29, wherein said security data is a digital certificate.

31.   (Previously Presented) The method according to claim 29, comprising reading said security data from the media peripheral.

32.   (Previously Presented) The method according to claim 29, comprising transferring said security data to a media exchange server coupled to the communication network.

33.   (Previously Presented) The method according to claim 29, comprising authenticating said acquired security data prior to said searching.

34.   (Previously Presented) The method according to claim 29, comprising, if said previously acquired security data is not found, establishing at least one identifier to

facilitate communication of the media peripheral over the communication network, wherein said at least one identifier is associated with the home; and

registering the media peripheral for operation in the home, based on said established at least one identifier.

35.   (Previously Presented) The method according to claim 29, wherein the communicated information comprises a previously established password.

36.   (Previously Presented) A system for establishing secure access to a media peripheral in a home via a node in a communication network, the system comprising:

at least one processor for use within the node, said at least one processor operable to acquire security data associated with the media peripheral;

said at least one processor operable to search for a previously acquired security data associated with a location of previous operation of the media peripheral;

said at least one processor operable to communicate between the node and the media peripheral, information associated with the media peripheral, while the media peripheral is located in the home, if said previously acquired security data is not found; and

said at least one processor operable to utilize said acquired security data associated with the media peripheral and said previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network, if said previously acquired security data is found;

said at least one processor operable to acquire at least one identifier associated with a location of previous operation of the media peripheral;

said at least one processor operable to validate said acquired at least one identifier based on said previously acquired security data, prior to communicating over the communication network; and

said at least one processor operable to register the media peripheral for subsequent operation while being located in the home.

37.   (Previously Presented) The system according to claim 36, wherein said security data is a digital certificate.

38.   (Previously Presented) The system according to claim 36, wherein said at least one processor is operable to read said security data from the media peripheral.

39.   (Previously Presented) The system according to claim 36, wherein said at least one processor is operable to transfer said security data to a media exchange server coupled to the communication network.

40.   (Previously Presented) The system according to claim 36, wherein said at least one processor is operable to authenticate said acquired security data prior to said searching.

41.   (Previously Presented) The system according to claim 36, wherein, if said previously acquired security data is not found, said at least one processor is operable to:

establish at least one identifier to facilitate communication of the media peripheral over the communication network, wherein said at least one identifier is associated with the home; and

register the media peripheral for operation in the home, based on said established at least one identifier.

42.   (Previously Presented) The system according to claim 36, wherein the communicated information comprises a previously established password.

43.   (Previously Presented) The system according to claim 36, wherein said at least one processor is one or more of a computer processor, a media peripheral processor, a media exchange system processor and/or a media processing system processor.